

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. – 20. (cancelled)

21. (new) A method of transmitting a frame counter value from a first correspondent to a second correspondent in a data communication system, said first correspondent having a frame counter for generating said frame counter value, and said first correspondent further having a sequence counter for generating a sequence counter value, said frame counter value and said sequence counter value being stored in memory; said method comprising steps being performed by said first correspondent and comprising:

- transferring said frame counter value and said sequence counter value from said memory into a processing unit;

- calculating in said processing unit a compressed representation of said frame counter value by removing from said frame counter value a component equal to said sequence counter value; and

- generating and transmitting a message over a communication link to said second correspondent in said data communication system, said message comprising said sequence counter value and said compressed representation of said frame counter value;

whereby upon receipt of said message by said second correspondent, said second correspondent may uniquely recover said frame counter value from said sequence counter value and said compressed representation of said frame counter value in said message.

22. (new) The method according to claim 21 wherein said sequence counter updates said sequence counter value subsequent to the transmission of a message.

23. (new) The method according to claim 22 wherein said sequence counter updates said sequence counter value by:

- (a) transferring said sequence counter value from said memory into a processing unit;
- (b) incrementing said sequence counter value in said processing unit in a direction of counting; and
- (c) replacing said sequence counter value stored in said memory with said incremented sequence counter value.

24. (new) The method according to claim 22 wherein said frame counter updates said frame counter value by:

- (a) transferring said frame counter value and said sequence counter value from said memory into a processing unit;
- (b) calculating in said processing unit a next value in a direction of counting from said frame counter value that is congruent to the sequence counter value modulo the size of the sequence counter; and
- (c) replacing said frame counter value stored in said memory with said calculated next value.

25. (new) The method according to claim 24 wherein the size of the sequence counter is 256.

26. (new) The method according to claim 21 wherein said frame counter value is used by at least one of said first and second correspondents in a cryptographic operation.

27. (new) The method according to claim 26 wherein said sequence counter value is used by said first correspondent for matching said message with an acknowledgement of said message sent from said second correspondent.

28. (new) The method according to claim 21 wherein said frame counter value is uniquely recoverable from said message by concatenating said compressed representation of said frame counter value and said sequence counter value.

29. (new) The method according to claim 28 wherein said compressed representation of said frame counter value is three bytes in length.

30. (new) A method of transmitting frame counter values from a first correspondent to a second correspondent in a data communication system, said first correspondent having a frame counter for generating said frame counter values, and said first correspondent further having a sequence counter for generating sequence counter values, said method comprising steps being performed by said first correspondent and comprising:

- transmitting over a communication link to said second correspondent in said data system an initial frame counter value and an initial sequence counter value;

- subsequently generating and transmitting messages to said second correspondent, each of said messages comprising a sequence counter value, but not a frame counter value; whereby upon receipt of each of said messages by said second correspondent, said second correspondent may recover said frame counter value from said sequence counter value in said message and from a previously stored frame counter value;

- periodically generating and transmitting to said second correspondent a message comprising both a frame counter value and a sequence counter value, the periodicity being defined by a predefined criteria.

31. (new) The method according to claim 30 wherein said sequence counter updates said sequence counter value subsequent to the transmission of a message.

32. (new) The method according to claim 31 wherein said sequence counter updates said sequence counter value by:

- (a) transferring said sequence counter value from memory into a processing unit;

- (b) incrementing said sequence counter value in said processing unit in a direction of counting; and

- (c) replacing said sequence counter value in said memory with said incremented

sequence counter value.

33. (new) The method according to claim 31 wherein said frame counter updates said frame counter value by:

(a) transferring said frame counter value and said sequence counter value from memory into a processing unit;

(b) calculating in said processing unit a next value in a direction of counting from said frame counter value that is congruent to the sequence counter value modulo the size of the sequence counter; and

(c) replacing said frame counter value in said memory with said calculated next value.

34. (new) The method according to claim 33 wherein the size of the sequence counter is 256.

35. (new) The method according to claim 30 wherein at least one of said frame counter values is used by at least one of said first and second correspondents in a cryptographic operation.

36. (new) The method according to claim 35 wherein said sequence counter values are used by said first correspondent for matching said message with an acknowledgement of said message sent from said second correspondent.

37. (new) The method according to claim 30 wherein said predefined criteria are when a predetermined number of said messages comprising a sequence counter value, but not a frame counter value, are transmitted by said first correspondent.

38. (new) The method according to claim 37 wherein said predetermined number is in the range 2 to 10.

39. (new) The method according to claim 30 wherein said first correspondent monitors for an acknowledgement of receipt of said messages by said second correspondent, and said predefined criteria are when no acknowledgement is received.